



Billing Code: 4410-02 P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 004-2011]

Privacy Act of 1974; System of Records

AGENCY: Federal Bureau of Investigation, Department of Justice.

ACTION: Notice to amend system of records.

SUMMARY: The Federal Bureau of Investigation proposes to amend its Terrorist Screening Records System, JUSTICE/FBI-019, maintained by the Terrorist Screening Center, to add two new categories of individuals and their associated records, to add a new routine use and make modifications to existing routine uses, and to make several administrative modifications and updates throughout the notice. Public comment is invited.

DATES: In accordance with 5 USC 552a(e)(4) and (11), the public is given a 30-day period in which to comment. Therefore, please submit any comments by [insert date 30 days after Federal Register publication].

ADDRESSES: The public, Office of Management and Budget (OMB), and Congress are invited to submit any comments to the Department of Justice, ATTN: Privacy Analyst, Office of Privacy and Civil Liberties, National Place Building, 1331 Pennsylvania Avenue, NW., Suite 1000, Washington, DC 20530-0001, or by facsimile to 202-307-0693.

FOR FURTHER INFORMATION CONTACT: Meghann Van Horne, TSC Privacy Officer, Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001.

SUPPLEMENTARY INFORMATION:

JUSTICE/FBI-019, last published in full at 72 FR 47073 (Aug. 22, 2007), describes the Terrorist Screening Records System maintained by the Federal Bureau of Investigation (FBI) at the Terrorist Screening Center (TSC) and at facilities operated by other government entities. These records are used in screening operations to ensure the security of the United States. The FBI now proposes to add two new categories of individuals to the system whose records will be useful in screening operations: relatives, associates, or others closely connected with known or suspected terrorists who are excludable from the United States based on these relationships by virtue of Section 212(a)(3)(B) of the Immigration and Nationality Act, as amended, and individuals who were officially detained during military operations, but not as enemy prisoners of war, and who have been identified as possibly posing a threat to national security. This latter category of individuals is commonly referred to as Military Detainees. Excludable individuals under the first category may be lawful permanent residents of the United States. Individuals in the second category are unlikely to be lawful permanent residents of the United States and even less likely to be U.S. citizens. Nevertheless, out of an abundance of caution and because potentially the status of a military detainee may change over time, the FBI is including military detainee records in its Terrorist Screening Records Systems. In addition to adding the two new categories of individuals, the FBI is also adding a routine use, which will enable the FBI to share information about

individuals who are excludable from the United States by virtue of Section 212(a)(3)(B) of the Immigration and Nationality Act with the Department of State and the Department of Homeland Security for the purposes of carrying out the provisions of this Act. The FBI is making pertinent revisions in other parts of the system notice to reflect the addition of these categories of individuals. Additional modifications to Justice/FBI-019 include: updates to the system location, record access procedures, and procedures for contesting records; clarifications to existing categories of records in the system; updates to the authorities section to reflect new authorities; and additions or changes to more accurately describe the system's purpose and routine uses. The FBI is republishing the entire system of records notice for ease of reference to these changes.

In accordance with 5 U.S.C. 552a(r), the Department of Justice has provided a report to OMB and the Congress on the modification of this system of records.

Date: November 23, 2011_

Nancy C. Libin
Chief Privacy and Civil Liberties Officer
United States Department of Justice

JUSTICE/FBI-019

SYSTEM NAME:

Terrorist Screening Records System (TSRS).

SECURITY CLASSIFICATION:

Classified and unclassified.

SYSTEM LOCATION:

Records described in this notice are maintained at the Terrorist Screening Center, Federal Bureau of Investigation, Washington, DC, and at facilities operated by other government entities for terrorism and national security threat screening, system back-up, and continuity of operations purposes.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

a. Individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (“known or suspected terrorists”);

b. Individuals, who are lawful permanent resident aliens but who are excludable from the United States based on their familial relationship, association, or connection with a known or suspected terrorist and who do not meet any of the applicable exceptions as described in Section 212(a)(3)(B) of the Immigration and Nationality Act of 1952 (hereinafter INA exceptions);

c. Individuals who were officially detained during military operations, but as not Enemy Prisoners of War, and who have been identified to pose an actual or possible threat to national security (hereinafter military detainees);

- d. Individuals who are the subject of queries against TSC information systems;
- e. Individuals identified during a terrorism screening process as a possible identity match to a known or suspected terrorist and other individuals who accompany or travel with such individuals;
- f. Individuals who are misidentified as a possible identity match to a known or suspected terrorist (“misidentified persons”);
- g. Individuals about whom a terrorist watchlist-related redress inquiry has been made; and
- h. Individuals whose information is collected and maintained for information system user auditing and security purposes, such as individuals who are authorized users of TSC information systems.

CATEGORIES OF RECORDS IN THE SYSTEM:

- a. Identifying biographical information, such as name, date of birth, place of birth, passport and/or drivers license information, biometric information, such as photographs and fingerprints, and other available identifying particulars used to compare the identity of an individual being screened, with a known or suspected terrorist, an INA exception, or a military detainee, including audit records containing this information;
- b. Information about encounters with individuals covered by this system, such as date, location, screening entity, analysis, associated individuals, and results (positive or negative identity match), and, for encounters with a known or suspected terrorist, INA exceptions, and military detainees only, other entities notified and details of any law enforcement, intelligence, or other operational response;

c. For a known or suspected terrorist, military detainee, or an INA exception, in addition to the categories of records listed above, references to and/or information from other government law enforcement and intelligence databases, or other relevant databases that may contain terrorism information;

d. For an individual considered to pose an actual or possible threat to national security, in addition to the categories of records listed above, references to and/or information from other government law enforcement and intelligence databases, or other relevant databases that may contain information related to possible threats to national security;

e. For misidentified persons, in addition to the categories of records listed above, other identifying information that will be used during screening only for the purpose of distinguishing them from a known or suspected terrorist, an INA exception, or a military detainee, any of whom may have similar identifying characteristics (such as name and date of birth);

f. For redress matters, in addition to the categories of records listed above, information provided by individuals or their representatives, information provided by the screening agency, and internal work papers and other documents related to researching and resolving the matter;

g. Information collected and compiled to maintain an audit trail of the activity of authorized users of TSC information systems, such as user name/ID, date/time, search query and results data, user activity information (e.g., record retrieval, modification, or deletion data), and record numbers; and,

h. Archived records and record histories from the Terrorist Screening Database, Encounter Management Application, and other TSC data systems that are part of the TSRS.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Homeland Security Presidential Directive-6, “Integration and Use of Screening Information to Protect Against Terrorism” (Sept. 16, 2003); Homeland Security Presidential Directive-11, “Comprehensive Terrorist-Related Screening Procedures” (Aug. 27, 2004); National Security Presidential Directive-59/Homeland Security Presidential Directive-24, “Biometrics for Identification and Screening to Enhance National Security” (June 5, 2008), (HSPD-24 gives the Attorney General authority to recommend categories of individuals in addition to known or suspected terrorists who may pose a threat to national security.); Executive Order 13388, “Further Strengthening the Sharing of Terrorism Information to Protect Americans,” (October 25, 2005); the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108–458; the National Security Act of 1947, as amended; 28 U.S.C. 533; and Section 212(a)(3)(B) of the Immigration and Nationality Act of 1952. In the event that the TSC’s continuity-of-operations plans are invoked, the agency that assumes TSC operational functions will have the authority to administer the Terrorist Screening Records System as necessary to carry out those functions.

PURPOSE(S):

a. To implement the U.S. Government’s National Strategy for Homeland Security and Homeland Security Presidential Directive-6, to identify potential terrorist threats, to uphold and enforce the law, and to ensure public safety.

b. To consolidate the government's approach to terrorism and national security screening and provide for the appropriate and lawful use of terrorist information and other lawfully acquired information in screening processes.

c. To implement the U.S. Government's Action Plan for National Security Presidential Directive-59/Homeland Security Presidential Directive-24, "Biometrics for Identification and Screening to Enhance National Security," to identify individuals considered to pose an actual or possible threat to national security.

d. To maintain current, accurate and thorough terrorist information and other lawfully acquired information in a consolidated terrorist screening database and determine which screening processes will use each entry in the database.

e. To ensure that appropriate information possessed by state, local, territorial, and tribal governments, which is lawfully available to the Federal Government, is considered in determinations made by the TSC as to whether a person is a match to a known or suspected terrorist, or a match to an individual considered to pose an actual or possible threat to national security.

f. To host mechanisms and make terrorism information, and information related to individuals considered to pose an actual or possible threat to national security, available to support appropriate domestic and foreign terrorism and national security screening processes, and private-sector screening processes that have a substantial bearing on homeland security.

g. To provide operational support to assist in the identification of persons screened and to facilitate an appropriate and lawful response when a known or suspected terrorist, or individual considered to pose an actual or possible threat to national security, is identified in an authorized screening process.

h. To provide appropriate government officials, agencies, or organizations with information about encounters with known or suspected terrorists or military detainees, INA exceptions or other individuals considered to pose an actual or possible threat to national security.

i. To assist persons misidentified during a terrorism screening process, or possible national security threat screening process, and to assist screening agencies or entities in responding to individual complaints about the screening process (redress).

j. To oversee the proper use, maintenance, and security of TSC data systems and TSC personnel.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, the records or information in this system may be disclosed as a routine use, under 5 U.S.C. 552a(b)(3), in accordance with blanket routine uses established for FBI record systems. See Blanket Routine Uses (BRU) Applicable to More Than One FBI Privacy Act System of Records, Justice/FBI-BRU, published at 66 FR 33558 (June 22, 2001) and amended at 70 FR 7513 (February 14, 2005). In addition, as routine uses specific to this system, the TSC may disclose relevant system records to the following

persons or entities and under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purpose for which the information was collected.

A. To those federal agencies that have agreed to provide support to TSC for purposes of ensuring the continuity of TSC operations.

B. To federal, state, local, tribal, territorial, foreign, multinational or other public agencies or entities, to entities regulated by any such agency or entity, and to owners/operators of critical infrastructure or private sector entities with a substantial bearing on national or homeland security and their agents, contractors or representatives, for the following purposes: (1) For use in and in support of terrorism screening, or possible national security threat screening, authorized by the U.S. Government, (2) to provide appropriate notifications of the results of terrorism screening, or possible national security threat screening, using information from the Terrorist Screening Database or a threat related to a positive encounter with an individual identified in the Terrorist Screening Database, (3) to facilitate any appropriate law enforcement or other response (e.g., medical and containment response to a biological hazard) to a known or suspected terrorist, an individual considered to pose an actual or possible threat to national security, or a threat related to an encounter with such an individual, and (4) to assist persons misidentified during a screening process.

C. To any person, organization, or governmental entity in order to notify them of a terrorist threat, or possible national security threat, for the purpose of guarding against or responding to such a threat.

D. To federal, state, local, tribal, territorial, foreign, or multinational agencies or entities, or other organizations that are engaged in, or are planning to engage in terrorism screening, or possible national security threat screening, authorized by the U.S. Government, for the purpose of the development, testing, or modification of information technology systems used or intended to be used during or in support of the screening process; whenever practicable, however, TSC, to the extent possible, will substitute anonymized or de-identified data, such that the identity of the individual cannot be derived from the data.

E. To federal, state, local, tribal, territorial, foreign, multinational agencies or entities, or private sector entities to assist in coordination of terrorist threat, or possible national security threat, awareness, assessment, analysis or response.

F. To any person or entity in either the public or private sector, domestic or foreign, where reasonably necessary to elicit information or cooperation from the recipient for use by the TSC in the performance of an authorized function, such as obtaining information from data sources as to the thoroughness, accuracy, currency, or reliability of the data provided so that the TSC may review the quality and integrity of its records for quality assurance or redress purposes, and may also assist persons misidentified during a screening process.

G. To any federal, state, local, tribal, territorial, foreign or multinational agency, task force, or other entity or person that receives information from the U.S. Government for terrorism screening purposes, or possible national security threat screening purposes,

in order to facilitate TSC's or the recipient's review, maintenance, and correction of TSC data for quality assurance or redress purposes, and to assist persons misidentified during a screening process.

H. To any agency, organization or person for the purposes of (1) performing authorized security, audit, or oversight operations of the DOJ, FBI, TSC, or any agency, organization, or person engaged in or providing information used for terrorism screening, or possible national security threat screening, that is supported by the TSC, and (2) meeting related reporting requirements.

I. To a former employee of the TSC for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with any applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the TSC requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

J. To any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, territorial, tribal, multinational or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

K. To a governmental entity lawfully engaged in collecting law enforcement, law enforcement intelligence, national security information, homeland security information, national intelligence, possible national security threat information, or terrorism information for law enforcement, intelligence, national security, homeland security, or counterterrorism purposes.

L. To appropriate agencies, entities, and persons when (1) the Department of Justice suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department of Justice has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department of Justice's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

M. To the United States Department of State and the United States Department of Homeland Security for the purpose of carrying out their responsibilities under Section 212(a)(3)(B) of the Immigration and Nationality Act of 1952.

DISCLOSURE TO CONSUMER REPORTING AGENCIES: None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:
STORAGE:

Records in this system are stored in paper and/or electronic format. Electronic storage is on servers, CD-ROMs, DVD-ROMs, and magnetic tapes.

RETRIEVABILITY:

Records in this system are typically retrieved by individual name, date of birth, passport number, and other identifying data, including unique identifying numbers assigned by the TSC or other government agencies.

SAFEGUARDS:

All records are maintained in a secure government facility with access limited to only authorized personnel or authorized and escorted visitors. Physical security protections include guards and locked facilities requiring badges and passwords for access. Records are accessed only by authorized government personnel and contractors and are protected by appropriate physical and technological safeguards to prevent unauthorized access. All Federal employees and contractors assigned to the TSC must hold an appropriate security clearance, sign a non-disclosure agreement, and undergo privacy and security training.

RETENTION AND DISPOSAL: Records in this system will be retained and disposed of in accordance with the records schedule approved by the National Archives and Records Administration. In general, for records maintained in the Terrorist Screening Database, active records are maintained for 99 years and inactive (archived) records are maintained for 50 years. Records of possible encounters with individuals on the Terrorist Screening Database are maintained for 99 years. Records of redress inquiries and quality assurance matters are maintained for at least six years. Audit logs are maintained for 25 years and records of user audits are maintained for ten years.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Terrorist Screening Center, Federal Bureau of Investigation, FBI Headquarters, 935 Pennsylvania Avenue, NW., Washington, DC 20535– 0001.

NOTIFICATION PROCEDURE:

Because this system contains classified intelligence and law enforcement information related to the government's counterterrorism, law enforcement, and

intelligence programs, records in this system have been exempted from notification, access, and amendment to the extent permitted by subsections (j) and (k) of the Privacy Act. Requests for notification should be addressed to the FBI at the address and according to the requirements set forth below under the heading “Record Access Procedures.”

RECORD ACCESS PROCEDURES:

Because this system contains classified intelligence and law enforcement information related to the government’s counterterrorism, law enforcement and intelligence programs, records in this system have been exempted from notification, access, and amendment to the extent permitted by subsections (j) and (k) of the Privacy Act. A request for access to a non-exempt record shall be made in writing with the envelope and the letter clearly marked “Privacy Act Request.” Include in the request your full name and complete address. The requester must sign the request; and, to verify it, the signature must be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. You may submit any other identifying data you wish to furnish to assist in making a proper search of the system. Requests for access to information must be addressed to the Record Information Dissemination Section, Federal Bureau of Investigation, 170 Marcel Drive, Winchester, Virginia 22602 or faxed to 540-868-4992.

CONTESTING RECORD PROCEDURES:

Because this system contains classified intelligence and law enforcement information related to the government’s counterterrorism, law enforcement and

intelligence programs, records in this system are exempt from notification, access, and amendment to the extent permitted by subsections (j) and (k) of the Privacy Act (5 U.S.C. 552a). Requests for amendment should be addressed to the FBI at the address and according to the requirements set forth above under the heading “Record Access Procedures.” If, however, individuals are experiencing repeated delays or difficulties during a government screening process and believe that this might be related to terrorist watch list information, they may contact the Federal agency that is conducting the screening process in question (“screening agency”). The screening agency is in the best position to determine if a particular problem relates to a terrorist watch list entry or is due to some other cause, such as a criminal history, an immigration violation or random screening. Some individuals also experience repeated delays during screening because their names and/or other identifying data, such as dates of birth, are similar to those of known or suspected terrorists. These individuals, referred to as “misidentified persons,” often believe that they themselves are on a terrorist watch list, when in fact they only bear a similarity in name or other identifier to an individual on the list. Most screening agencies have or are developing procedures to expedite the clearance of misidentified persons during screening. By contacting the screening agency with a complaint, individuals will be able to take advantage of the procedures available to help misidentified persons and others experiencing screening problems. Check the agency’s requirements for submitting complaints but, at a minimum, individuals should describe in as much detail as possible the problem they are having, including dates and locations of screening, and provide sufficient information to identify themselves, such as full name, citizenship status, and date and place of birth. The TSC assists the screening agency in

resolving any screening complaints that may relate to terrorist watch list information, but does not receive or respond to individual complaints directly. However, if TSC receives any such complaints, TSC will forward them to the appropriate screening agency.

Additional information about the redress process and how to file a complaint with a screening agency is available on TSC's Web site at http://www.fbi.gov/about-us/nsb/tsc/tsc_redress.

RECORD SOURCE CATEGORIES:

Information in this system is obtained from individuals covered by the system, public sources, agencies and private sector entities conducting terrorism screening, law enforcement and intelligence agency record systems, government databases, and foreign governments.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d)(1), (2), (3) and (4), (e)(1), (2), (3), (5) and (8), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j) and (k).

These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and are located at 28 CFR 16.96.